CITY UNIVERSITY OF HONG KONG
Information Classification and Handling Standard

(Approved by the Information Strategy and Governance Committee in January 2023)

Document Control

Document Owner	Classification	Publication Date
OCIO	PUBLIC	2023-01-28

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2015-01-12	Replaced Data Owner by Information Owner or Owner Modified to allow Owners to share responsibilities with Delegates Modified Information Classification Matrix, to Disallow reuse of paper with “RESTRICTED”/ “CONFIDENTIAL” info; Remove mandatory use of registered mail, required to mark envelope with proper label Remove need for signing NDA for sharing of INTERNAL information Clarify the requirement of password handling for sending “RESTRICTED”/”CONFIDENTIAL” attachment over email.
1.2	2023-01-28	Revised the link and reference material in this document.

Distribution

Copy	Issued to	Location
Master	Public	https://www.cityu.edu.hk/cio/information-security/information-security-policies-and-standards

Contents

1 Policy Statement

Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. The City University of Hong Kong ("University") shall classify, label and handle information resources based on their sensitivity, criticality, value, nature and impact of unauthorized disclosure in accordance with legal, regulatory and contractual requirements. This standard outlines the specific requirements and guidelines for the implementation of Section 4 – "Information Classification and Handling" in "Information Security Policies".

2 Objective

The objective of this Information Classification and Handling Standard is to provide guidance on how the information should be handled in accordance with its classification standard. All the University members that may come into contact with such information shall familiarize themselves with this information classification standard and follow it consistently.

3 Scope

This Information Classification and Handling Standard applies to the electronic data and printed documents stored in any form within the University or in relation to the University.

4 Information Identification

Before establishing security controls, the Information Owner/Delegate must identify and classify information assets to be protected. The "Information & IT Asset Inventory and Ownership Standard" provides guidance on how assets should be identified and registered.

5 Information Classifications

The University must classify all its information assets into appropriate levels to indicate the need, priority and degree of protection required.

When handling personal data, the personal data user must ensure compliance with the Personal Data (Privacy) Ordinance, and the University's "Code of Practice for Personal Data (Privacy) Issues".

Research data and research information are important assets to the University. The University shall protect the confidentiality and integrity of research data and research information without creating unjustified obstacles to research activities. Information related assets funded by research grants shall also conform to the "Policies and Guidelines relating to Research" maintained by Research Grants and Contracts Office of the University.

The degree of protection required for different types of information is based on security and legislative compliance requirements. The following four classification levels, from highest to least, shall be used for classifying the University's information assets.

If information has not been marked with one of the following categories, the Information Owner/Delegate must initiate the data classification process and assign appropriate classification levels timely.

5.1 RESTRICTED

This classification applies to the information that is very sensitive in nature and is strictly confidential to the University, the government or any other agreements between the University and third parties (including the government).

Such information is considered critical to the University's capacity to conduct its business. Generally, this information shall be used exclusively by a small number of predetermined and authorized named individuals, roles or positions and business partners.

Either disclosure of it to unauthorized parties or being shared internally could have significant adverse impact on the University's reputation, its staffs, students and third parties. Inappropriate release of "**RESTRICTED**" information could cause unforeseeable damage to or endanger an individual, and result in financial lost or damage to standing or reputation at University level.

Examples of information with this classification include:

- examination papers before being released,
- privileged accounts' passwords of the University's key information systems
- pending criminal investigation

"**RESTRICTED**" and "**SECRET**" used interchangeably in the scope of this set of Information Security Policies and Standards. "**RESTRICTED**" is the preferred classification label. Existing information classified as "**SECRET**" should be reclassified into "**RESTRICTED**" upon review of classification.

5.2 CONFIDENTIAL

This classification applies to sensitive information that is intended for use by specific group of authorized personnel within the University and business partners, assigned on a need-to-use basis and for authorized intended purpose.

The unauthorized disclosure, modification or destruction of this information would adversely affect the business performance or the continuity of operations. Inappropriate release of "CONFIDENTIAL" information could cause inconvenience to individuals, and result in limited financial lost or damage to a standing or reputation at unit level.

Information of interest for news media, pressure group or electorates is also classified as "CONFIDENTIAL".

Such information shall not be copied or removed from the University's control without specific authorization.

Examples of information with this classification include:

- student information (e.g., student HKID, credit card information)
- staff information (e.g., staff HKID, personal financial or medical information)

- student and staff disciplinary details
- patent pending
- unpublished research information
- Identifiable research subject data

5.3 INTERNAL

This classification related to non-sensitive operational data. It applies to information that is intended for use within by members of the University and authorized services providers. Disclosure of such information could have moderate adverse impact. Disclosures are not expected to cause serious harm to the University and access may be provided freely to a specific group of staffs based on their roles and responsibilities. Examples of information with this classification include University's staff handbooks, policies, training materials, manuals, procedures, etc.

5.4 PUBLIC

This classification applies to information that has been approved by authorized parties for public consumption. Public information shall present no perceived risk to the University, its staff and/or students. Examples of information with this classification include program and admission information, published academic literature, press releases, address of a department, etc.

6 Responsibility

Information/System Owners/Delegates are responsible for identifying the classification level of information.

All staff members are responsible for handling information in accordance with this procedure.

Head of Departments of all University Units shall ensure their responsible areas' compliance to this procedure.

7 Labeling Information Assets

Information that is classified as "**RESTRICTED**", "**CONFIDENTIAL**" or "**INTERNAL**" should be appropriately labeled. Unlabeled emails are considered as "Internal", unlabeled information on other types of media is considered as "Public". Tabulated below are some common labeling methods for various types of information assets.

Information Types	Labeling Procedures
Hard copy documents	Define classification in Record Control Table[1], header or footer. Place identification if document classified as "**RESTRICTED**", "**CONFIDENTIAL**" or "**INTERNAL**".

[1] Refer to Appendix A for a sample of "Record Control Table".

Electronic mail	All emails are for the use of intended recipient only, and shall not be classified as "**PUBLIC**". Email sent using "University account" and "Supplementary account" of the University are classified as "**INTERNAL**" by default. Indicate classification in subject line of email or classification field, if classified as "**RESTRICTED**" or "**CONFIDENTIAL**".
Electronic documents	Place information classification mark on top/bottom of electronic documents if classified as "**RESTRICTED**", "**CONFIDENTIAL**" or "**INTERNAL**", or register the classification in the Record Control Table.
Data, databases and business applications	Define classification in system/application metadata or Record Control Table. Labels may be required for reports generated by IT systems if classified as "**RESTRICTED**", "**CONFIDENTIAL**" or "**INTERNAL**"
Other media	If classified as "**RESTRICTED**", "**CONFIDENTIAL**" or "**INTERNAL**", identify classification on adhesive labels applied to other media such as diskettes, CDs, DVDs, and videocassettes; and a message with the classification label may be displayed when the information stored on the media is accessed.

8 Information Handling

8.1 Handling of "RESTRICTED" or "CONFIDENTIAL" Information

The University shall not remove or forward **RESTRICTED** or **CONFIDENTIAL** information from its premises unless prior approval from the Information Owners/Delegates has been obtained. This standard includes portable computers with hard disks, CDs, USB, floppy disks, hardcopy outputs, paper memos and the likes. An exception is made for authorized off-site backups. An audit trail must log all attempts (successful or unsuccessful) to access **RESTRICTED** information.

8.2 Storage and Transmission of "RESTRICTED" or "CONFIDENTIAL" Information

The University shall ensure that the storage media is physically secured. Storage and transmission of **RESTRICTED** or **CONFIDENTIAL** information at rest or over communications networks shall be encrypted.

Wherever possible, the University shall implement encryption and password control over the storage or media containing **RESTRICTED** or **CONFIDENTIAL** information in accordance with the requirement stipulated in "Logical Access Control Security Standard".

8.3 Re-classification of Information

The University's Information Owners/Delegates are required to re-classify the classification of information when warranted within a reasonable time. Based on the classification criteria mentioned in Section 5 "Information Classifications", the information can be re-classified to a different level. For example, financial data before it is released may be classified as **CONFIDENTIAL** or **INTERNAL**. Once the data are made public, such as published in journals, examinations, and quarterly or annual reports, it should be re-classified as **PUBLIC**.

8.4 Release of RESTRICTED, CONFIDENTIAL or INTERNAL Information to Third Parties

The University shall ensure that all **RESTRICTED**, **CONFIDENTIAL** or **INTERNAL** information is protected from disclosure to third parties by default. Exceptions are permissible if the release of this information is clearly needed to accomplish a certain objective of the University based on the principles of purpose, reasonableness and non-excessiveness, and if the identity of the receiving party has first been confirmed. The Information Owners/Delegates needs to establish requirements for any disclosures of **RESTRICTED**, **CONFIDENTIAL** or **INTERNAL** information to third parties. Any disclosures of the University's **RESTRICTED** or **CONFIDENTIAL** information to third parties must be subject to a written agreement specifying what information is restricted and how this information may and may not be used. Consent from the Information Owners/Delegates must be sought prior to the release of **RESTRICTED** or **CONFIDENTIAL** information to third parties.

8.5 Retention and Disposal of Information

Every member of the University has the responsibilities to consider security when using and disposing of information in all circumstances.

Departments or contractors that are regarded as key Information Owners/Delegates or Controllers/Custodians shall be responsible for defining and documenting the retention period of critical data. The legal requirements and responsible parties should also be specified.

University shall define appropriate retention periods for certain kinds of information. Every department or contractor should establish procedures appropriate to the information held and processed by them, and ensure that all relevant parties are aware of those procedures.

Departments or contractors must retain records and information if:

1. they are likely to be needed in the future, unless a specific retention cycle has already mandated by specific policy to ensure their availability timely, such as the existing policy on email retention.
2. regulation or statute requires their retention, or
3. they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts or to allow the University to respond to discovery requests, subpoenas, investigatory demands and other requests for information related to legal or regulatory proceedings.

Sensitive information should be disposed of according to the respective disposal procedures for different classifications of information in order to ensure complete removal of **RESTRICTED**, **CONFIDENTIAL** or **INTERNAL** information, including both paper based and electronic forms. Disposal procedures include shredding, low level formatting, degaussing of hard disk drives etc.

Unauthorized destruction or disposal of the University's sensitive information will subject the perpetrator to disciplinary action including termination and prosecution.

Please refer to Section 9 for detailed handling procedures for each type of classification.

8.6 Backup and Recovery

The University must implement the same level of security measures for the backup of **RESTRICTED**, **CONFIDENTIAL** and **INTERNAL** information.

Backup procedures shall be documented and in accordance with the security requirement for handling of **RESTRICTED**, **CONFIDENTIAL** and **INTERNAL** information. In particular, the following details shall be specified:

- Backup Scope (i.e. category and classification of information to be backed up);
- Backup Frequency;
- Backup Media;
- On-site and/or Off-site Backup Location;
- Backup Retention;
- Logical and Physical Security Measures for Backup Media and Location; and
- Backup Method (i.e. Incremental, Differential or Full).

Request to restore **RESTRICTED**, **CONFIDENTIAL** and **INTERNAL** information from backup media must be approved by IT Management and respective Information Owners/Delegates. The University must restrict the access to the restored data to authorized members.

Backup and recovery of **RESTRICTED**, **CONFIDENTIAL** and **INTERNAL** information must be performed by authorized IT operational staff and audited by independent parties at least annually.

Please refer to Section 9 for detailed handling procedures for each type of classification.

9 Information Classification Matrix

The following table identifies handling procedures for information in the various classification categories.

	RESTRICTED	CONFIDENTIAL	INTERNAL	PUBLIC
Disclosure	By permission of Info Owners/Delegates only; Strictly for work purpose only		Need-to-know basis	No concern
Copying Hard Copy or Electronic Media	Approval from Info Owners/Delegates required		No concern	
Removal from University premises	Approval from Info Owners/Delegates required		No concern	
Protected Storage (online and backup) on fixed electronic media[2] (see note 3)	Masked/Encrypted with access control and password control required	Access control and password control required; Masked/Encrypted recommended	Access control and password control required	Access control and password control for Create/ Update/ Delete
Desktop Storage on Fixed Electronic Media (see note 3)	Encrypted with "Strong" password. Desktop protected with appropriate controls		Desktop protected with appropriate controls	
Use/Store on Mobile Computing Devices[3]	Approval from Info Owners/Delegates required; Password protection and encryption are required; Erase data after 10 failed passcode attempt recommended	Approval from Info Owners/Delegates required; Password protection and encryption are required	Password protection is required	No concern
Portable Storage (e.g. DVD, tapes, disks, USB drive)	Approval from Info Owners/Delegates required; Encrypted with "Strong" password, stored in locked secured places		Stored in locked secured places	No concern
Disposal of material media (e.g. DVD, Printed copy)	Shredding		Shredding recommended	No concern

[2] Protected storage are secured by additional layers for security controls, e.g. physically locked in a secure locked in a secured room such as data center and locked store room, and electronically protected by additional layers of firewall and IPS/IDS.

[3] Such as Smartphones (e.g. iPhone, Android based smartphones)

	RESTRICTED	CONFIDENTIAL	INTERNAL	PUBLIC
Disposal of digital media (e.g. tapes, disks, USB drive)	Degaussing, Wiping with three pass data overwriting[4]	Degaussing, Wiping with single pass data overwriting	Reformat required. Wiping with single pass data overwriting recommended	No concern
Email transmission	Encrypted attachment, password MUST NOT be distributed in the same email or sent from/to the same email accounts		No concern	
Material media transmission (e.g. DVD, Printed copy)	By hand or authorized courier service with acknowledgement Proper sealing and labeling required		Suitable cover or envelope	No concern
Fax transmission	Fax only after ensuring receiving party is secured			No concern
Postal transmission	Mark the envelope with proper label, e.g. “RESTRICTED”, ”CONFIDENTIAL”, “PRIVATE & CONFIDENTIAL” Registered mail recommended		No concern	
Release to 3rd parties	Approval from info owner required; NDS [5]must be signed	NDA must be signed	NDA Should be signed	No concern
Logging and Monitoring	Recipients, Copies, Made, Locations, Address, Those who Viewed and Destruction	Movement of electronic storage media containing personal identifiable information must be tracked	No concern	
Reuse of paper	Disallowed		Within same unit	No concern

Notes:

1. Various classes of information located in one common medium/location should have the highest classification of all information located in the medium.
2. For mail packaging and delivery, internal means within same office in the same building, whereas external means from office/location to any other different offices/locations, or to another building.
3. Fixed Electronic Media means storage devices embedded inside the equipment (e.g. servers, desktop computers, photocopiers, and digital multi-functional systems, etc.) and cannot be taken away without modification the equipment.
4. Portable Storage Media means media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the

[4] Refer to NIST 800-88 “Guidelines For Media Sanitization”

[5] Non-disclosure agreement

computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including notebook computers, hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial software disks.

10 Summary

To effectively protect the information assets the University must establish appropriate information classification scheme and clearly assign its members with the responsibilities towards secure information handling. Retention and disposal of information assets must be performed in accordance with the procedures defined by the key data custodians or owners.

Appendix A – Sample Record Control Table

Record Control Table				
Document ID	**Document / Record Name**	**Owner**	**Classification**	**Retention Period**
ISMS-ISPS-001	Information Security Policies	OCIO	INTERNAL	3 years
ISMS-ISPS-004	Information Classification and Handling Standard	OCIO	INTERNAL	3 years
n/a	Integrated Management System Database	OCIO ISU	CONFIDENTIAL	3 years

References

The following documents were consulted during the preparation of this document:

City University of Hong Kong, *Code of Practice for Personal Data (Privacy) Issues*, Version 18 (Last update: Nov 2021) https://www.cityu.edu.hk/vpad/ctu-only/code-of-practice.pdf

City University of Hong Kong, *University Policy on Intellectual Property and Related Matters*, Revised in Nov 2022, https://www.cityu.edu.hk/policies/ippolicy/about-the-policy

Carnegie Mellon University. (2021). *Guidelines for Data Classification*. Retrieved 7 Dec 2022, from http://www.cmu.edu/iso/governance/guidelines/data-classification.html

Duke University. (2014). *Data Classification* Standard. Retrieved 7 Dec 2022, from https://security.duke.edu/policies-procedures-and-standards/data-security/data-classification-standard/

Harvard University. (n.d.). *Research Data Security*. Retrieved 7 Dec 2022, from https://researchdatamanagement.harvard.edu/research-data-security

Johns Hopkins University. (2019). *Information Technology Policies*. Retrieved 7 Dec 2022, from http://www.it.johnshopkins.edu/policies/itpolicies.html

Princeton University. (2020). *Information Security Policy*. Retrieved 7 Dec 2022, from https://oit.princeton.edu/policies/information-security

Queensland Government. (2020). *Information security classification framework (QGISCF)* Retrieved 7 Dec 2022, from https://www.qgcio.qld.gov.au/documents/information-security-classification-framework-qgiscf

Stanford University. (2015). *Risk Classifications* Retrieved 7 Dec 2022, from https://uit.stanford.edu/guide/riskclassifications

Yale University. (2018). *1604 Data Classification Policy* Retrieved 7 Dec 2022, from https://your.yale.edu/policies-procedures/policies/1604-data-classification-policy